REMARKS

As a preliminary matter, Applicant notes that claim 3 has been amended to correct a minor typographical error not noted by the Examiner. No new matter has been added.

The present invention is directed to a system that provides security for a protected function. In one embodiment, a wireless communications device stores an authorization code in memory. The authorization code may be provided by a central controller, and is based on a master code stored at the central controller. To gain access to a protected function (e.g., unlocking a locked door), the wireless communications device transmits an access request to an access control device associated with the door (e.g., a door lock). The access control device responds by transmitting an authentication challenge to the wireless communications device. Based on both the authentication challenge and the authentication code stored in memory, the wireless communications device **computes** an authentication response and returns the response to the access control device. If the access control device recognizes the authentication response as valid, the user gains access to the protected function (e.g., the door is unlocked).

The Examiner maintains the rejection of claim 1 under 35 U.S.C. §103 in view of Henderson (U.S. Patent No. 5,602,536). Henderson discloses a system and method by which users may gain access to real estate lock boxes. The system of Henderson includes a lockbox, a key, and a stand to provide the key and the lockbox with a variety of data. According to Henderson, the lockbox and the key operate responsive to the exchange of signals between the two. More particularly, the key sends an interrogation signal to the lockbox to wake up the lockbox system. In response, the lockbox sends a response signal to the key, where the second signal comprises lockbox battery information and date information. If the key has not expired relative to the date provided by the lockbox, the key sends an identification signal to the lockbox. By comparing the identification signal to stored identification information, the lockbox determines if the key has permission to open the lockbox.

Contrastingly, claim 1 requires that the wireless communication device implement the steps of "storing an authorization code... receiving an authentication challenge from said access control device ... [and] computing an authentication response based on said authentication challenge and said authorization code." The Examiner concedes that Henderson does not teach the concept of "authentication challenge" in the sense of the claim. However, the Examiner contends that it would have been obvious to modify the Henderson security system to include a known authentication-type security feature, such as a password feature. In particular, the Examiner asserts that receiving a request for a password corresponds to receiving an authentication challenge, and providing a password corresponds to providing an authentication response.

First, the proposed modification does not solve the deficiencies of Henderson. Nothing in a conventional password-type authentication system satisfies the computing step of claim 1. Password-type authentication systems simply require users or devices to provide a known password in response to a password request. Contrastingly, claim 1 requires that the wireless communication device compute a response to the authentication challenge based on the challenge sent by the access control device and the authentication code stored in the wireless communication device, and to provide the computed response in response to the authentication challenge. Nothing in Henderson, as modified by the Examiner, teaches or suggests a key that computes any type of response, much less a response based on an authentication challenge and a stored authentication code. As such, even when modified as suggested by the Examiner, Henderson does not teach each and every limitation of claim 1.

Second, Applicant notes that there is no motivation for modifying Henderson as suggested by the Examiner. The key in Henderson provides all of the necessary security in the context of Henderson. Nothing in Henderson indicates that additional password security is useful or desired. As such, there is no motivation to modify Henderson as suggested by the Examiner. In fact, the Examiner does not even provide any motivation as to why the skilled user

would modify Henderson to include a password-type authentication system. Instead, the Examiner simply asserts that password authentication systems are well known, and therefore, it would be obvious to modify Henderson to include such a system. Simply because a reference can be modified does not mean there is motivation to do so. *In re Laskowski*, 871 F.2d 115, 117 (Fed. Cir. 1989); *In re Gordon*, 733 F.2d 900, 902 (Fed. Cir. 1984). For at least these reasons, the obviousness rejection of claim 1 is legally insufficient and must be withdrawn.

In addition, the Examiner also rejects independent claims 15, 40, and 60 under 35 U.S.C. §103(a) as unpatentable over Henderson for the same reasons as those cited above for claim 1. Claim 40, however, claims a device that comprises "a processor to compute to compute said authentication response based on said authentication challenge received from said access control device and said authorization code." Claims 15 and 60 claim the access control device that receives the authentication response, but require that the authentication response be based on the authentication challenge and an authorization code stored in memory of the wireless communications device. Therefore, for reasons similar to those stated above, Henderson also fails to teach or suggest any of independent claims 15, 40, and 60.

The Examiner also maintains the rejection of independent claims 36 and 72 under 35 U.S.C. §103(a) as being unpatentable over Wang. In the pending office action, the Examiner neglected to respond to Applicants arguments regarding the Wang reference and simply restated the rejection. Should the Examiner again maintain this rejection, Applicants request the Examiner explicitly address Applicants patentability arguments, which are repeated below for the Examiner's convenience.

Claim 36 is directed to a central controller that computes the authentication code for the wireless communications device responsive to an initialization request received from the wireless communications device. The Examiner admits that Wang does not teach or suggest "initialization" as recited in claim 36. While this is true, there is an even more glaring deviation.

Notably, Wang does not teach or suggest a central controller that "[computes] an authorization code based on [a] master code ... in response to receipt of [an] initialization request."

Wang discloses a system that is used in Point-Of-Sale (POS) operations. In Wang, a server may transmit a transaction program (TP) to a user's Portable Electronic Authorization Device (PEAD). The TP includes an executable portion that may comprise sets of codes. Far from being an authorization code, however, these codes are used by the PEAD to encrypt data that approves a POS transaction. *Wang*, col. 3, ll. 24-32. Additionally, the codes may be used to search a user's computing device for the PEAD (i.e., to detect the presence of the PEAD), or to query for and retrieve user identification information from the user's device. *Wang*, col. 16, ll. 7-33. Wang does not teach or suggest that a central controller computes an authorization code for the user based on a master code. Nor does Wang teach or suggest that the device receives an authorization code. In fact, Wang does not teach or suggest that the server even has a master code. As such, Wang fails to teach or suggest each of the limitations of claim 36.

Claim 72 recites language similar to that recited in claim 36. Therefore, for the reasons stated above with respect to claim 36, Wang also fails to teach or suggest claim 72.

While the dependent claims are patentable because their corresponding independent claims are patentable, as discussed above, Applicants also note that the rejections of most of the dependent claims are legally insufficient. First, in rejecting claims 3 – 4, 6 – 11, 15 – 35, 40 – 50, 54 – 56, and 60 – 71, the Examiner simply broadly asserts that "such particular features are well known in the art for the purpose of handling information across processing systems and for the purpose of security." In addition, the Examiner says nothing at all about the rejection of dependent claims 37 – 39 and 72 – 77. Such unsupported assertions and/or rejections do not satisfy the requirements of MPEP 2142, which requires the Examiner to present convincing reasoning as to why the claimed limitations are obvious in view of any cited art. As such, the rejections are legally insufficient and must be withdrawn.

Even when the Examiner provides support for a rejection of a dependent claim, the rejection is incomplete. For example, each of claims 2 – 4, 18 – 21, 42 – 43, and 62 - 64 require generating the authorization code based on a combination of a secret code and a time indication. In supporting the rejection against claim 2, the Examiner contends that providing a time indication to limit access to a secure device is well known in the art. However, claim 2 requires "generating an authorization code based on a combination of a secret code and a time indication to limit access to said protected function to a defined time period" (emphasis added). Because the Examiner ignores the fact that the authorization code is based on the secret code as well as the time indication, the rejection is legally insufficient and must be withdrawn. Similar logic applies to claims 3 – 4, 18 – 21, 42 – 43, and 62 – 64.

In light of the forgoing remarks, Applicants respectfully request reconsideration of the rejections and allowance of all pending claims 1-77. Should any issues remain unresolved, Applicants request the Examiner call the undersigned so that such issues may be resolved expeditiously.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

Dated: 22 June 2005

Jennifer K. Stewart
Registration No.: 53,639

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844